Sentinel Agent Manager

Migration Guide

February 2015

Contents

Security Manager customers migrating to Sentinel can leverage their Security Manager Windows, UNIX, and iSeries agent deployments to provide host-based data collection with Sentinel.

This Migration Guide provides information about migrating Security Manager agents to a Sentinel environment with Sentinel Agent Manager installed.

Overview

Migrating from Security Manager to Sentinel Agent Manager allows you to leverage your existing Security Manager environment, and the time you have invested in it, by migrating Security Manager Windows, UNIX, and iSeries agents for use with Sentinel Agent Manager.

The host-based data collection offered by Sentinel Agent Manager complements traditional Sentinel data collection by allowing you to:

- Access logs not available from the network
- Operate in tightly-controlled network environments
- Improve security posture by limiting attack surface on critical servers
- Provide enhanced reliability of data collection during times of network interruption

Specifying that you want to migrate Security Manager agents to Sentinel during the Sentinel Agent Manager installation allows Sentinel Agent Manager to easily access agent information by installing the Agent Manager databases on the same SQL server instance as the Security Manager database. This allows the Agent Migration Tool to easily re-assign Windows, UNIX, and iSeries agents to Sentinel Agent Manager central computers without requiring changes to the individual agents.

Once agents begin communicating with a Sentinel Agent Manager central computer, the agent no longer uses Security Manager rules or content. Instead, Sentinel Agent Manager uses data collection policies to collect and forward events to Sentinel. At this time, you can take full advantage of all of Sentinel's capabilities.

What Sentinel Provides

The Sentinel Web console now provides the following functionality you are used to seeing in Security Manager for host-based data collection:

- Computer Views
- Computer Group Views
- Infrastructure Views
- Computer Group Definitions
- Attribute Definitions

The following table maps Security Manager features that are replaced by corresponding features in Sentinel.

Table 1 *Security Manager to Sentinel Agent Manager Feature Map*

Security Manager Feature	Sentinel Feature
Event Views	Pre-defined search filters
Alert Views	Incidents
Forensic Analysis	Reports and Searches
Trend Analysis	Security Intelligence
Incident Packages	Incidents
My Views	Pre-defined search filter

What Sentinel Agent Manager Provides

Sentinel Agent Manager provides the following functionality you are used to seeing in Security Manager:

- Log Collection Rules
- Data Provider Configuration
- Global Windows Agent Configuration
- Agent Administrator

Assessing Your Environment

To help plan your transition from monitoring agents with Security Manager to monitoring agents with Sentinel, review the following environment considerations before migrating your agents.

Migrating in Phases

To provide flexibility in planning when you want to migrate your Security Manager Windows, UNIX, and iSeries agents, Security Manager continues to collect event data until the agent has been reassigned to a Sentinel Agent Manager central computer. This ongoing monitoring allows you to migrate your agents in phases while minimizing downtime and helping to prevent data loss.

Repurposing Security Manager Central Computers

If you want to leverage existing hardware in your environment, you can repurpose an existing Security Manager central computer for use with Sentinel. Once you have migrated all agents off of a Security Manager central computer, you can repurpose the computer for use as a Sentinel Agent Manager central computer.

For example, if you have two Security Manager central computers, both of which monitor two agents, you can temporarily migrate all four agents to a Sentinel Agent Manager central computer in your environment. When the Security Manager central computer no longer monitors agents, you can repurpose it as a Sentinel Agent Manager central computer. You can then reassign two of the agents to send data to your repurposed central computer.

To repurpose the Security Manger central computer:

1. Temporarily migrate all agents from the central computer for which you want to repurpose the computer as a Sentinel Agent Manager central computer.
2. When the Security Manager central computer no longer monitors agents, uninstall the Security Manager central computer.
3. Install a Sentinel Agent Manager central computer on the computer where you uninstalled the Security Manager central computer.
4. From the Agent Manager console, access Agent Administrator.
5. Assign agents to the repurposed central computer.

Multiple Configuration Groups

The Agent Migration Tool supports migrating agents from a single configuration group. If you have more than one configuration group in your environment you need to install a Sentinel server for each configuration group.

To ensure minimal downtime and to avoid data loss, Security Manager agents support both Security Manager and Sentinel Agent Manager central computers. While you migrate agents from one configuration group to a Sentinel Agent Manager central computer, the other configuration group continues managing the agents using the Security Manager infrastructure until the agent migration is successful.

User-Defined Computer Groups

If you created custom computer groups to group Windows computers based on specified criteria, such as domain, or operating system, you must use the Sentinel Web console to re-create these computer groups and attribute definitions. The Agent Migration Tool does not retain user-defined computer groups or computer attribute definitions.

Proxy Agents

If you use proxy agents to remotely monitor and collect events from an agentless monitored computer, you can configure Sentinel to monitor these computers using Connectors and Collectors. For example, the Windows Event (WMI) Connector includes a proxy that can query WMI, fetch Windows events, and pass them to a Collector. Sentinel Agent Manager does not support agentless monitoring. For more information about using Connectors and Collectors for data collection, see the *Sentinel Installation Guide*.

Product Requirements

To migrate agents from Security Manager to Sentinel Agent Manager, you must have the following software installed and configured in your environment:

- Sentinel
- Sentinel Agent Manager
- Security Manager
- Security Manager agents

For information about installing Sentinel, see the *Installation Guide for Sentinel*. For information about installing Sentinel Agent Manager, see the *Installation Guide for Sentinel Agent Manager*. For information about upgrading Security Manager agents, see the *Installation Guide for Security Manager*.

Migrating Security Manager Agents to Sentinel

To migrate Windows, UNIX, or iSeries managed and unmanaged agents to Sentinel, use the Agent Migration Tool to reassign an agent from Security Manager to a Sentinel Agent Manager central computer. The migration process can take 15 to 30 minutes for each agent. Once you have successfully migrated an agent, it can take an additional 15 to 30 minutes for Sentinel to display events

To migrate Security Manager agents to Sentinel:

1. Log on to the Sentinel Agent Manager computer with an account that is a member of the OnePointOp ConfgAdms group. For more information about groups and permissions, see the *User Guide for Sentinel Agent Manager*.
2. Start the Agent Migration Tool from the NetIQ Sentinel Agent Manager program group.
3. Follow the instructions in the Agent Migration Tool to migrate your Windows, UNIX, and iSeries agents in the specified configuration group.
4. Review the status of the migrated agents.
5. (Conditional) If you migrated UNIX agents, use UNIX Agent Manager to configure the migrated agents to not send real-time data to a Sentinel Agent Manager central computer.
6. (Conditional) If you migrated iSeries agents, use iSeries controls to configure the migrated agent to send iSeries Notification Events to a Sentinel Agent Manager central computer.

7 (Conditional) If you used custom computer groups and attribute definitions for the agents you migrated, use the Sentinel Web console to re-create these computer groups and attribute definitions.

8 Review Terminology Updates to understand how Security Manager concepts are described in Sentinel Agent Manager and Sentinel documentation.

Agent Migration Status

Use the following migration status descriptions to evaluate the state of your Sentinel Agent Manager migration and to troubleshoot any migration attempts that were not successful.

Table 2 *Agent Migration Status*

Migration Status	Description
Not Migrated	The Migration Tool has not migrated the agent and it is still managed by Security Manager.
Not Migrated, Agent Offline	The Migration Tool has not migrated the agent and it is still managed by Security Manager; however, the agent has not recently contacted Security Manager and may be offline or otherwise non-functional. You need to bring the agent back online before you can migrate the agent.
Not Migrated	The Migration Tool has not migrated the agent and it is still managed by Security Manager. If the agent is a Security Manager legacy agent (pre-6.5.x), you must upgrade the agent to Security Manager 6.5 before you can migrate the agent.
Migration In Progress	Agent migration has been initiated, but the agent has not yet contacted Agent Manager. Migration normally takes two to four heartbeat intervals, where heartbeat intervals are five minutes, by default.
Migration Failed	Agent migration has been initiated, but the agent failed to communicate with Sentinel Agent Manager within two “Display agent status unknown” intervals. Each interval is 10 minutes by default. Information about why the migration failed is in the Agent Details. When an agent is in the Migration Failed state, you can select a new Sentinel Agent Manager central computer to which you want to migrate.
Migration Complete	The agent has been successfully migrated and is now managed by and receives configuration information from the Sentinel Agent Manager infrastructure. The agent no longer communicates with the Security Manager infrastructure.

Terminology Updates

The following table provides a list of updated terminology used in Sentinel Agent Manager.

Table 3 *Security Manager to Sentinel Agent Manager Terminology Mapping*

Security Manager term	Sentinel Agent Manager term	Description
Processing Rule Group	Data Collection Policies	Identifies a particular log source from which to collect data. This configuration includes information about the type of log source, such as File or Event Log, and information to locate the log source. Data Collection Policies also allow data to be excluded from collection using Filter Rules.
Log Collection Rule	Data Collection Rule	Identifies the events to collect from logs across the network. Sentinel Agent Manager collects only events that match a data collection rule.
Computer Group	Device Group	Identifies a collection of computers with something in common, such as a group of all computers with Norton AntiVirus installed. Sentinel Agent Manager deploys data collection policies assigned to a device group.
Computer Rule	Device Group Definition	Identifies a logical expression built from Device Attribute definitions used to define a set of computers with similar characteristics or purpose.
Computer Attribute	Device Attribute Definitions	Identifies a collection of values that identify computer attributes, such as the operating system or installed applications.